Gröbner Basis and deducibility

Charlie Jacomme

July 13, 2018

LSV & LORIA[a]

[a] CNRS, INRIA, ENS Paris-Saclay

Introduction to security

A rising need for security

$$\text{Confidentiality:} \quad \begin{cases} \text{Banking operations} \\ \text{Smartphones with GPS} \\ \dots \end{cases}$$

A rising need for security

$$\text{Confidentiality:} \quad \begin{cases} \text{Banking operations} \\ \text{Smartphones with GPS} \\ \dots \end{cases}$$

$$\text{Authentication:} \quad \begin{cases} \text{Internet shopping} \\ \text{Private emails} \\ \dots \end{cases}$$

Cryptographic primitives

A public encryption scheme:

Cryptographic primitives

A public encryption scheme:

- A public key *pk*
- A secret key *sk*

Cryptographic primitives

A public encryption scheme:

- A public key pk
- A secret key sk
- An encryption function $enc(message, pk)$
- A decryption function $dec(cypher, sk)$

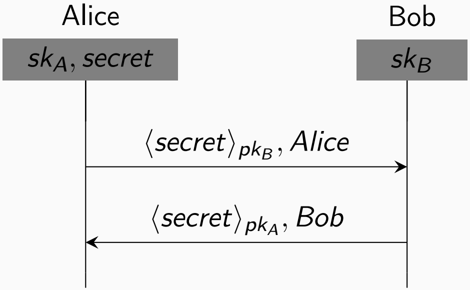
Cryptographic primitives

A public encryption scheme:

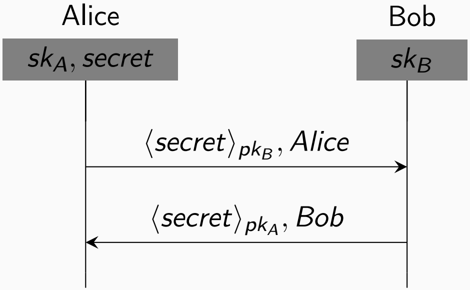
- A public key *pk*
- A secret key *sk*
- An encryption function $enc(message, pk)$
- A decryption function $dec(cypher, sk)$

based on exponentiation in group and hardness of discrete logarithm

Protocols

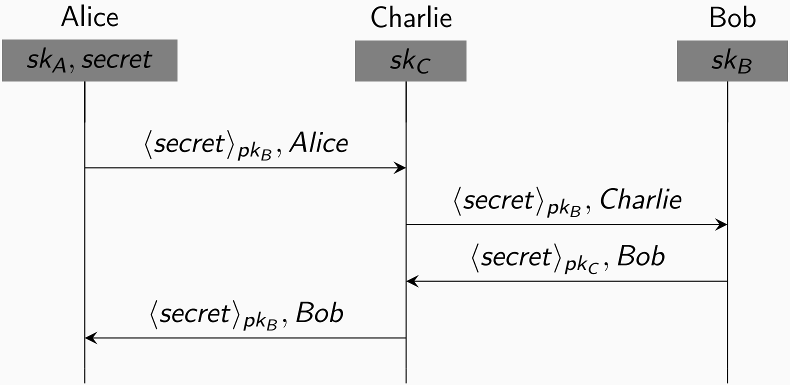

Alice
Bob
$sk_A, secret$
sk_B
$\langle secret \rangle_{pk_B}, Alice$
$\langle secret \rangle_{pk_A}, Bob$

Protocols



Is secret secret ?

Protocols



No !

Formal methods

Proofs of security are

- difficult
- error prone

Formal methods

Proofs of security are

- difficult
- error prone

$\hookrightarrow$ We want automation

Deducibility

Deducibility

Deducibility

Given a set of messages, can an attacker deduce a secret ?

Deducibility

Deducibility

Given a set of messages, can an attacker deduce a secret ?

Messages are

- $x, y, z, \dots$ random variables over $\mathbb{K}$
- g^f with $f \in \mathbb{K}[X]$

Deducibility

Given a set of messages, can an attacker deduce a secret ?

Messages are

- $x, y, z, \ldots$ random variables over $\mathbb{K}$
- g^f with $f \in \mathbb{K}[X]$

Example

$$x, g^{x \times y}, g^{y^2} \vdash g^{y^2+y}$$

Deducibility

Deducibility

Given a set of messages, can an attacker deduce a secret ?

Messages are

- $x, y, z, \ldots$ random variables over $\mathbb{K}$
- g^f with $f \in \mathbb{K}[X]$

Example

$$x, g^{x \times y}, g^{y^2} \vdash g^{y^2+y}$$

$$g^{y^2+y} = (g^{x \times y})^{x^{-1}} \times g^{y^2}$$

Our generalized problem

$$\Gamma \models X, g^{f_1}, ..., g^{f_k} \vdash g^h \qquad \begin{cases} \Gamma \text{ axioms} \\ X \text{ public variables} \\ Y \text{ secret variables} \\ g \text{ group} \\ f_i, h \text{ polynomials over } \mathbb{K}[X, Y] \end{cases}$$

The algorithm

$$\Gamma \models X, g^{f_1}, \ldots, g^{f_k} \vdash g_t^h$$

With Gröbner Basis

The algorithm

$$\Gamma \models X, g^{f_1}, ..., g^{f_k} \vdash g_t^h$$

With Gröbner Basis

1. Characterize the attacker knowledge:

$$M = \{\sum_i e_i \times f_i | e_i \in \mathbb{K}[X]\}$$

The algorithm

$$\Gamma \models X, g^{f_1}, ..., g^{f_k} \vdash g_t^h$$

With Gröbner Basis

1. Characterize the attacker knowledge:

$$M = \{\sum_i e_i \times f_i | e_i \in \mathbb{K}[X]\}$$

2. Saturate using the axioms, if $\Gamma = \{p_k \neq 0\}$:

$$M :_{\mathbb{K}[X,Y]} (p_1 ... p_n)^\infty = \{f \in \mathbb{K}[X, Y] | \exists n \in \mathbb{N}, f \times (p_1 ... p_n)^n \in M\}$$

The algorithm

$$\Gamma \models X, g^{f_1}, ..., g^{f_k} \vdash g_t^h$$

With Gröbner Basis

1. Characterize the attacker knowledge:
$$M = \{\sum_i e_i \times f_i | e_i \in \mathbb{K}[X]\}$$
2. Saturate using the axioms, if $\Gamma = \{p_k \neq 0\}$:
$$M :_{\mathbb{K}[X,Y]} (p_1...p_n)^\infty = \{f \in \mathbb{K}[X, Y] | \exists n \in \mathbb{N}, f \times (p_1...p_n)^n \in M\}$$
3. Test the membership.

Gröbner Basis

(in)Formal definition

For f, g_i in $\mathbb{K}[X, Y]$, we have:

- an ordering on monomials
- if $lm(f) = qlm(g_1)$ then $red_1^X(f, g_1) = f - qg$
- $red^X(f, g_i)$ is the iteration of red_1 for all g_i

(in)Formal definition

For f, g_i in $\mathbb{K}[X, Y]$, we have:

- an ordering on monomials
- if $lm(f) = qlm(g_1)$ then $red_1^X(f, g_1) = f - qg$
- $red^X(f, g_i)$ is the iteration of red_1 for all g_i

Gröbner Basis

$$G = \{g_i\} \text{ is a GB pf } M \text{ iff } \forall h \in M, red(h, G) = 0$$

Buchberger's algorithm

For f, g_i in $\mathbb{K}[X, Y]$, we have:

$$S(f, g_1) = \frac{lppcm(f, g_1)}{lm(g)} f - \frac{lppcm(f, g_1)}{lm(f)} g$$

Buchberger's algorithm

For f, g_i in $\mathbb{K}[X, Y]$, we have:

$$S(f, g_1) = \frac{lppcm(f, g_1)}{lm(g)} f - \frac{lppcm(f, g_1)}{lm(f)} g$$

Given $G = \{g_i\}$:

- compute a $S(g_i, g_j)$
- reduce it w.r.t to G
- if its remainder is non zero, add it to G

Buchberger's algorithm

For f, g_i in $\mathbb{K}[X, Y]$, we have:

$$S(f, g_1) = \frac{lppcm(f, g_1)}{lm(g)} f - \frac{lppcm(f, g_1)}{lm(f)} g$$

Given $G = \{g_i\}$:

- compute a $S(g_i, g_j)$
- reduce it w.r.t to G
- if its remainder is non zero, add it to G

Saturation

Goal

If $M =< G >$, compute the GB of

$$M :_{\mathbb{K}[X,Y]} (p)^{\infty} = \{f \in \mathbb{K}[X,Y] | \exists n \in \mathbb{N}, f \times (p)^n \in M\}$$

Saturation

Goal

If $M =< G >$, compute the GB of

$$M :_{\mathbb{K}[X,Y]} (p)^{\infty} = \{f \in \mathbb{K}[X,Y] | \exists n \in \mathbb{N}, f \times (p)^n \in M\}$$

Magic trick

- compute the GB of $G \cup (1 - tp)$, with t a fresh variable
- keep only the base element not containing t.

The algorithm

$$\Gamma \models X, g^{f_1}, ..., g^{f_k} \vdash g^h$$

With Gröbner Basis

1. Characterize the attacker knowledge:

$$M = \{\sum_i e_i \times f_i | e_i \in \mathbb{K}[X]\}$$

2. Saturate using the axioms, if $\Gamma = \{p_k \neq 0\}$:

$$M :_{\mathbb{K}[X,Y]} (p_1 ... p_n)^\infty = \{f \in \mathbb{K}[X, Y] | \exists n \in \mathbb{N}, f \times (p_1 ... p_n)^n \in M\}$$

3. Test the membership.

Conclusion

Conclusion

It is a good idea to to have general knowledge in math when doing computer science !